УДК 003.26.09

АНАЛИЗ АЛГОРИТМОВ ВЫЧИСЛЕНИЯ ТОЧКИ КРАТНОСТИ 5 ЭЛЛИПТИЧЕСКОЙ КРИВОЙ TWISTED EDWARDS

Долгов Д.А.

ФГАОУ ВПО Казанский (Приволжский) федеральный университет, 420008, г. Казань, ул. Кремлевская, д.18.

e-mail: dadolgoff@yandex.ru

поступила в редакцию 13 сентября 2013 года

Аннотация

Бернштейн и Ланге получили новый вид кривой, $E_{E,a,d}$ Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2$. В рамках данной статьи рассматриваются алгоритмы вычисления кратных точек для кривой Twisted Edwards.

Ускорение операций вычисления кратных точек ЭК упрощает реализацию многочисленных алгоритмов шифрования и ЭЦП в криптографии. Новые алгоритмы работают лучше, быстрее, эффективнее, что позволяет расширить область их использования – ЭЦП цифровых сообщений, SMS, надежная аутентификация сообщений и т.п, что позволит построить более защищенные коммерческие продукты.

Ключевые слова: *эллиптические кривые, Twisted Edwards, конечные поля, криптография, кратные точки.*

Введение. В 1985 году Коблиц и Миллер предложили использовать в криптографии алгебраические свойства эллиптических кривых. В криптографии эллиптических кривых роль основной криптографической операции играет скалярное умножение точки данной кривой на целое число, которые выполняются на основе операций сложения, умножения и инвертирования. Ленстра представил алгоритм факторизации целых чисел за время $\exp(\sqrt{2} + o(1)\sqrt{p\ln(p)\ln(\ln p)})$. Долгое время использовались кривые Вейерштрасса $E_{W,k}$: $y^2 = x^3 + ax + b$, над конечным полем F_k $k \neq 2;3$. Позднее Монтгомери предложил новую форму эллиптической кривой $Bv^2 = u^3 + Au^2 + u$, над полем $F_k, k \neq 2;3$. Новая форма позволила уменьшить время факторизации. Основные улучшения алгоритма Ленстры связаны с поиском новых видов кривых, позволяющих минимизировать вычисление кратных точек.

Основная часть. В [1] доказано, что формулы для 3P,5P выполняются быстрее.

$$3P \le 2P + P \quad 3P \le 4P - P$$

$$5P \le 2 * 3P - P \quad 5P \le 2 * 2P + P$$

Twisted Edwards:Новые формулы для 3P,5P точек

Вычислении точек кратности 3 :

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; D = A + B; $E = D^2$; F = 2D · (A − B); K=4C; L = E − B· K; M = E - AK; N = F + M; $X_3 = 2L * P * X_1$; $Y_3 = M * ((N + Y)^2 - O - B)_1$; $Z_3 = P((N + Z_1)^2 - O - C)$;

Вычислении точек кратности 5 :

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; D = A + B; E = 2C − D; F = A*A; $G = B^2$; $H = F + G$; $I = D^2 - H$; J = E*E; K = G − F; L = K · K; M = 2*I*J; N = L+M; O = L-M; P = N · O; $Q = (E + K)^2 - J$; $R = ((D + E)^2 - J - H - I)^2 * 2N$; S = QP; T = 4QO(D-C);

U=R*N; V=U+T; W=U-T; $X_5 = 2X_1 * (P + B * S) * W$. $Y_5 = 2Y_1 * (P - A * S) * V$; $Z_5 = Z_1 * V * W$.

Экспериментальная часть. Производилась оценка новых формул по сравнению с формулами из [1]. У [1] теоретическая оценка была 17M+ 7S, у новых формул- 14M+11S. Очевидно, в среднем случае [1] эффективнее. Но при разложении, когда S/M<1/3 получается, что новые формулы эффективнее в среднем на 10% (рисунки 1 и 2).

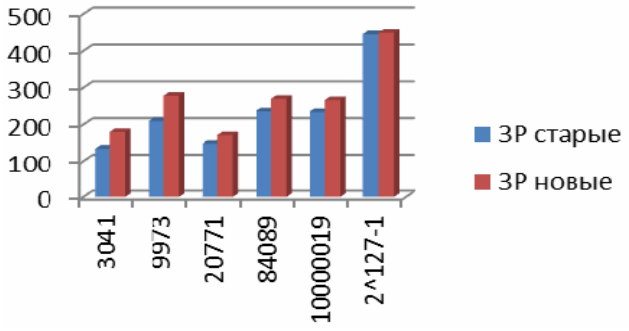

Рисунок 1. – Сравнение формул для 3P.

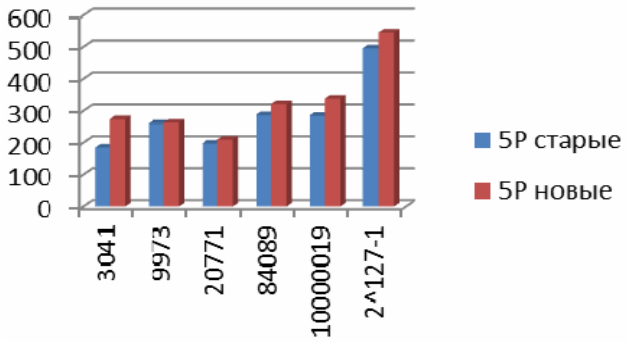

Рисунок 2. – Сравнение формул для 5P.

Вычисление кратной точки. NextPoint5PNeighbour и NextPoint5PBase. Сравнение проводится с алгоритмом NextPoint5P из [1]. В основе лежат алгоритмы суммирования и удвоения, а также наиболее новые формулы 3P, 5P, в случае, если выполняется, что S/M<1/3. Иначе используются старые формулы.

NextPoint5PNeighbour. Идея проста: на каждой итерации происходит поиск ближайшего значения. Так как в памяти хранится история вычислений, то нет необходимости производить старые вычисления заново.

Цикл:

While(true):

- Узнать ближайшего соседа слева, справа: $t \in \left\{5^k, 2*5^k, 3*5^k, 5^{(k+1)}\right\}$, где достигается min abs(n-t), $k = \left[\log_5 m\right]$
- Вычислить $tZ * (-1^{n-t})$, разложение t уже знаем $n = n - 5^{[\log_5 n]} * (-1^{n-t})$.
- T=T+kZ.
- n==0? Выход.

NextPoint5PBase. Идея проста: на каждой итерации происходит поиск ближайшего значения относительно базы предвычисленных значений. Это помогает найти наиболее близкого соседа числа.

1. Цикл:

While(true):

- Узнать ближайшего соседа min abs(n-t), t ∈ DB[1]

- Вычислить $tZ*(-1^{n-t})$, разложение t уже знаем $n = n - 5^{[\log_5 n]}*(-1^{n-t})$.
- T=T+kZ.
- n==0? Выход.

В трех случаях мы имеем одинаковую худшую оценку. Но в среднем, новые алгоритмы получаются более эффективными за счет наилучшего разложения кратности точки.

Таблица 1. – Сравнение алгоритмов разложения точек кратности 5.

Метод[2]	Теоретическая оценка	Средний % выигрыша к алгоритму NextPoint5P
Edwards NextPoint5PBase	$\lceil \log_5 n \rceil 5P + 2(\lceil \log_5 n \rceil 1)\, Double$ $+(\lceil \log_5 n \rceil - 1)\, Addition$	20%
Edwards NextPoint5P nearest neighbour	$\lceil \log_5 n \rceil 5P + 2(\lceil \log_5 n \rceil 1)\, Double$ $+(\lceil \log_5 n \rceil - 1)\, Addition$	10%

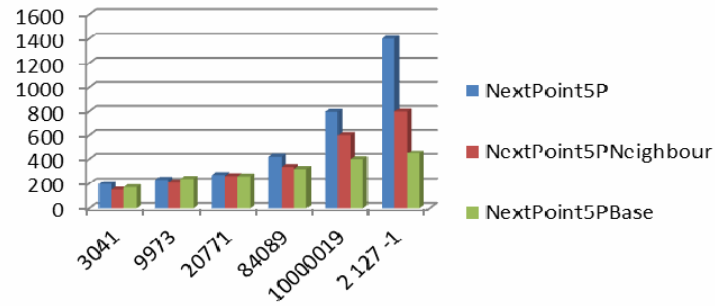

Рисунок 3. – Сравнение алгоритмов.

Заключение. Новые формулы 3P,5P доказали свою эффективность для формул, в которых число операций умножения превосходит число операций сложения не менее, чем в 3 раза. Алгоритм NextPoint5PBase показал в среднем 20% выигрыш по отношению к алгоритму NextPoint5P (рисунок 3, таблица 1). Он является наиболее эффективным алгоритмом на сегодняшний день.

Список литературы

1) Долгов Д. Сравнительный анализ вычисления кратных точек на эллиптических кривых вида Montgomery, Weierstrass, Twisted Edwards // Труды 4 Всероссийской конференции «Информационные технологии в системе Социально-экономической безопасности России и ее регионов». 2012. 153 с.
2) Долгов Д. Анализ алгоритмов поиска кратности точки эллиптической кривой // Труды Научно-образовательной конференции студентов КФУ. 2013.
3) Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. Казань: Изд. КФУ. 2011. 210 с.
4) Долгов Д. Эффективный алгоритм вычисления кратных точек на эллиптических кривых вида Weierstrass, Montgomery, Twisted Edwards // Труды конференции «Туполевские чтения». 2012.
5) Bernstein D., Birkner P., Lange T., Peters C. Twisted Edwards Curves // Abstract of the First international conference on cryptology in Africa. Casablanca, Morocco, June 11-14. 2008. P.389-405.

[1] База предвычисленных значений
[2] Для случайных кривых над проективными координатами.